# SECURITY IN ROBOT OPERATING SYSTEM (ROS) BY USING ADVANCED ENCRYPTION STANDARD (AES)

NOR ALIA SYUHADA BINTI SHAHARUDIN

Bachelor of Computer Science (Computer Systems & Networking)

UNIVERSITI MALAYSIA PAHANG

## SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree in Bachelor of Computer Science (Computer Systems & Networking)

(Supervisor's Signature)

Full Name : DR LUHUR BAYUAJI

Position : SENIOR LECTURER

Date : 24 DECEMBER 2018

## STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : NOR ALIA SYUHADA BINTI SHAHARUDIN

ID Number : CA15073

Date : 24 DECEMBER 2018

# SECURITY IN ROBOT OPERATING SYSTEM (ROS) BY USING ADVANCED ENCRYPTION STANDARD (AES)

NOR ALIA SYUHADA BINTI SHAHARUDIN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Science (Computer Systems & Networking)

Faculty of Computer Systems & Sofware Engineering

UNIVERSITI MALAYSIA PAHANG

DECEMBER 2018

## ACKNOWLEDGEMENTS

I would like to express my appreciation to my supervisor, Dr. Luhur Bayuaji for his guidance during this research is conducted. Without his valuable assistance, this thesis would not have been completed.

In addition, I also would like to thank to all the people around me who involve directly or indirect in completing this research. I also appreciate all the moral support and courage that has been given to me from my family members and friends who always be there to help me finishing this research as well as to those who sacrifice their time to help me improve and complete this research.

Finally, I would like to thanks to the staff of the Faculty of Computer Systems & Software Engineering for their valuable assistance during the development of this thesis.

# ABSTRAK

Oleh kerana system robotik semakin tersebar, siber sekuriti muncul sebagai tumpuan utama. Pada masa kini, kebanyakan sistem autonomi dibina menggunakan rangka ROS yang merupakan rangka yang paling popular untuk membangunkan aplikasi robotik bersama dengan perisian komersil yang lain. ROS adalah rangka kerja yang diedarkan di mana nod menerbitkan maklumat yang digunakan oleh nod lain. Model ini memudahkan komunikasi data tetapi menimbulkan ancaman utama kerana proses yang berniat jahat boleh mengganggu komunikasi dengan mudah, membaca mesej peribadi, atau mengambil alih pergerakan robot. Kajian ini menyiasat prestasi robot apabila memecahkan mesej yang ditukar antara nod ROS di bawah paradigma menerbitkan/melanggan. Khususnya, kajian ini memberi tumpuan kepada penggunaan algoritma penyulitan iaitu AES. Algoritma penyulitan akan dinilai berdasarkan prestasi sistem, baik dari sudut pengkomputeran dan juga komunikasi.

## ABSTRACT

As robotic systems spread, cybersecurity emerges as major concern. Currently, most research autonomous systems are built using the ROS framework which has become the most popular framework for developing robotic applications along with other commercial software. ROS is a distributed framework where nodes publish information that other nodes consume. This model simplifies data communication but poses a major threat because a malicious process could easily interfere the communications, read private messages, or even take over the robots movement. The study investigates a robot's performance when ciphering the messages interchanged between ROS nodes under the publish/subscribe paradigm. In particular, this research focuses on using encryption algorithm which is AES. The encryption algorithm will be evaluated according to the performance of the system, both from computing and communications point of view.

## TABLE OF CONTENT

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| 3DES | Triple DES |
| AES | Advanced Encryption Standard |
| CBC | Cipher Block Chaining |
| CFB | Cipher Feedback |
| CTR | Counter |
| DoS | Denial of Service |
| ECB | Electronic Code Book |
| OFB | Output Feedback |
| ROS | Robot Operating System |

# CHAPTER 1

# INTRODUCTION

## 1.1 Background of Study

In current world growing technology, robots become more sophisticated and it have a high demand in fields such as medical, construction, military as well as household robots. Robots are playing an important role for human that can affect our daily lives. National security and defense are now depend on drones. Amazon use robots to distribute their supply chain and goods. Surgical robots that is operated remotely by the surgeon will likely to be used in more scenarios such as emergency response and military. Automated vehicles are being developed by companies like Google and Tesla. An analysis of 280 companies that was carried out by Department of Commerce on Competitiveness showed an average rate growth of 62% in the healthcare and eldercare markets as well as 20% average growth rate for robotics use in manufacturing, service and medical fields (Dorsey, Martin, Howard, & Coovert, 2017). Based on this data, it proves that the use of the robots is increasing and will be likely to contribute more in the future.

Robotics systems are growing not just in the virtual world, science-fiction movies, but also in our normal life. It is possible to find driverless cars in the streets, autonomous robotic guides at museums and the most common is autonomous vacuum cleaners in our homes. These robotic systems can suffer from different types of cyber-attack, hence some standard of cybersecurity is enforced.

The widely known framework for developing robotic applications is ROS (Robotic Operating System) that controls the autonomous behaviour of the robots. ROS is an emerging standard for creating a new robots application in the future, but it is not

immune to cyber-attack or hacking. Therefore, it is important for the ROS framework to be more secured to avoid security problem.

## 1.2 Problem Statement

Generally, robots are created to provide service to people, hence the human robot interaction is important. It can obtain user's information in a blink of eye with the advancement of technology in the last few decades. Service robots may one day also collect data and information about the health and wellbeing of the person that it serves. The data that non-authorized and suspicious entitiy gained will let them to misuse it for their own benefit. The robots also can be controlled if outsider able to enter the system of the robots.

ROS is a distributed framework where nodes publish information that other nodes consume. The message-passing distribution between the nodes in ROS was implemented in plain text. It simplifies data communication but poses major threat because malicious process could easily interfere the communications and read private messages. Therefore, cryptography technique such as Advanced Encryption Standard (AES) must be implemented in publisher and subscriber nodes to protect the confidentiality, integrity and availability of the data.

In addition, cryptography is an important technology that able to protect information against the outsider such as suspicious users and adversaries. The fundamental issue in plotting and designing an encryption algorithm must be the security of the algorithm against undesirable attack. AES have three different length of keys which is 128, 192 and 256 bits. The differences in key length will present different performance. Hence, AES with different key length is analysed in order to choose which algorithm is better for ROS framework.

## 1.3 Objective

Based on the problems statement, the objectives of this research are:

i. To identify the possible cyber security attack that can occur in Robot Operating System (ROS).
ii. To implement the AES algorithm with different key length in the communication of ROS.
iii. To evaluate the performance of AES algorithm based on the system parameter in ROS.

## 1.4 Scope

The study focus on comparison between different length of keys in AES algorithm in the security of robots based on ROS. The purpose of the algorithm is to improve the security of the communication in ROS. The scope also includes the user such as researchers and organizations. The main software that is used in this research is ROS Indigo.

## 1.5 Thesis Organization

The thesis consists of five chapters. The organization and flow of the thesis is as follows. Chapter 1 shall discuss on introduction to the research. In the second chapter, literature review of the research is discussed. In Chapter 3, the methodology used is interpreted. Chapter 4 are literally about the implementation and result discussion. Lastly, Chapter 5 contains the conclusion of the research findings.

# REFERENCES


Abdulazeez, A. M., & Tahir, A. S. (2015). Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA, (September 2013).

Adenowo, A. A. A., & Adenowo, B. A. (2013). Software Engineering Methodologies: A Review of the Waterfall Model and Object-Oriented Approach. *International Journal of Scientific & Engineering Research*, *4*(7), 427–434. Retrieved from http://www.ijser.org/researchpaper%5CSoftware-Engineering-Methodologies-A-Review-of-the-Waterfall-Model-and-ObjectOriented-Approach.pdf

Bhanot, R., & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms, *9*(4), 289–306.

Bonaci, T., Yan, J., Kohno, T., & Chizeck, H. J. (2015). To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots, (April).

Denning, T., Matuszek, C., Koscher, K., Smith, J. R., & Kohno, T. (2009). A Spotlight on Security and Privacy Risks with Future Household Robots : Attacks and Lessons, (October 2014). https://doi.org/10.1145/1620545.1620564

Dorsey, D. W., Martin, J., Howard, D. J., & Coovert, M. D. (2017). Cybersecurity issues in selection. *Handbook of Employee Selection, Second Edition*, 913–929. https://doi.org/10.4324/9781315690193

Hwang, M., & Liu, C. (2005). Authenticated Encryption Schemes : Current Status and Key Issues, *1*(2), 61–73.

Krovetz, T., & Rogaway, P. (2011). The Software Performance of Authenticated-Encryption Modes, *2011*(Fse), 1–24.

Morante, S., Victores, J. G., & Balaguer, C. (2015). Cryptobotics : why robots need cyber safety, *2*(September), 23–26. https://doi.org/10.3389/frobt.2015.00023

Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., … Mg, A. (2009). ROS: an open-source Robot Operating System. *Icra*, *3*(Figure 1), 5. https://doi.org/http://www.willowgarage.com/papers/ros-open-source-robot-operating-system

Rodr, F. J., Casado, F., Fern, C., & Mart, F. (2016). Cybersecurity in Autonomous Systems : Evaluating the performance of hardening ROS, (June), 47–53.

ROS_Introduction - ROS Wiki. (n.d.).

ROS_Tutorials_WritingPublisherSubscriber(python) - ROS Wiki. (n.d.).

Santos, M. A., Pereira, S., & Couceiro, M. S. (n.d.). On the Security of Robotic Applications Using ROS, 273–289.

Shirabadagi, S. S., & Nadagoud, S. (2017). A new encryption methodology of aes algorithm using high speed s-box, *4*(7), 37–42.

Stallings, W. (n.d.). *D ATA AND C OMPUTER*.